

We claim:

1. An improved method of electronic voting over a global computer network comprising the steps of:

requesting a voting ballot through a voting entity process using a public key and a private key of the voting entity;

validating said voting ballot request by a voting mediator, using a separate public key and private key of the voting mediator;

generating an electronic ballot by the voting mediator;

sending the generated ballot to said voting entity;

receiving a vote in said electronic ballot by said voting entity and sending said electronic ballot to a voting tabulator; and

counting the vote electronic ballot in the voting tabulator.

2. The method of claim 1 wherein said ballot requesting step further comprises:

obtaining a voting certificate from the voting mediator;

extracting the voting mediator's public key from the voting certificate;

encrypting the ballot request with the voting mediator's public key.

3. The method of claim 2 further comprising the step of packaging said ballot request within a sealed object, said sealed object comprising a signature of the data, voting certificate and an encryption of the sealed objects.

4. The method of claim 3 further comprising the step of signing said ballot request with voting entity's private key and sending said ballot request to the voting mediator.

5. The method of claim 4 further comprising the steps of:

receiving said ballot request by the voting mediator;

decrypting the encrypted ballot request with said voting mediator's private key;

validating said voting entity's certificate; and

authenticating and verifying the integrity of signed ballot request using the public key within said voting entity's certificate.

6. The method of claim 5 further comprising the step of authorizing a ballot request by checking the signing certificate information against the appropriate database; and determining whether said voting entity has previously voted in the identified election.

7. The method of claim 5 wherein the voting mediator validates said ballot request by ensuring that the validity period of the voting certificate has not expired, that the certificate can be traced to a root certificate and that the public key of the voting mediator validates the signature on the certificate

8. The method of claim 7 further comprising the step of ensuring that said ballot request comes from the voting entity requesting the ballot by extracting a public key from the voting entity's certificate and using the voting entity's public key to validate the signature of the signed ballot request.

9. The method of claim 1 wherein said ballot generating step further comprises the step of authorizing said ballot request by said voting mediator, said authorizing step comprising creating an electronic ballot having the unique election identification information and ballot number.

10. The method of claim 9 further comprising the steps of obtaining the public key of the voting tabulator and encrypting said generated ballot with said voting tabulator's public key before sending said signed and encrypted ballot to said voting entity.

11. The method of claim 1 further comprising before step (e) the step of receiving the signed and encrypted message containing the electronic ballot by said voting entity, decrypting the signed and encrypted message with the voting entity's private key to extract the information contained in the message and validating the signed message with said voting mediator's public key.

12. The method of claim 1 wherein the voting tabulator tabulates votes comprising the steps of:

- receiving an encrypted voting information message;
- inspecting the ballot contained in the message to ensure that votes are for the election the voting tabulator is tabulating;
- requesting ballot validation from the voting mediator; and
- tabulating votes from the received ballot.

13. The method of claim 12 wherein the voting mediator receives said validation request and decrypts and validates the ballot request to determine ballot validity.

14. The method of claim 13 further comprising the steps of:

- sending signal and encrypted ballot validation to the voting tabulator by the voting mediator; and
- receiving this response at the voting tabulator and validating and decrypting the response and verifying the validation response.

15. A system for implementing an electronic voting process over a global computer network comprising:

- a voting entity said voting entity being a client process representing a person or group that will be voting in the election;
- a voting mediator said voting mediator being a server process that authorizes and creates the anonymous electronic ballot for the voting entity; and
- a voting tabulator said voting tabular being a server process that receives and validates the electronic ballot and tabulates the election results.

16. The architecture of claim 15 wherein each said voting entity, voting mediator and voting tabulator has a separate public key and private key.

17. A computer program product in a computer readable medium for electronic voting over a global computer network, the computer program product comprising:

instructions for requesting a voting ballot through a voting entity process using a public key and a private key of the voting entity;

instructions for validating said voting ballot request by a voting mediator, using a separate public key and private key of the voting mediator;

instructions for generating an electronic ballot by the voting mediator;

instructions for sending the generated ballot to said voting entity;

instructions for receiving a vote in said electronic ballot by said voting entity and sending said electronic ballot to a voting tabulator; and

instructions for counting the vote electronic ballot in the voting tabulator.

18. The computer program product as described in claim 17 wherein said ballot requesting instruction further comprises:

instructions for obtaining a voting certificate from the voting mediator;

instructions for extracting the voting mediator's public key from the voting certificate;

instructions for encrypting the ballot request with the voting mediator's public key.

19. The computer program product as described in claim 18 further comprising an instruction for packaging said ballot request within a sealed object, said sealed object comprising a signature of the data, voting certificate and an encryption of the sealed objects.

20. The computer program product as described in claim 19 further comprising an instruction for signing said ballot request with voting entity's private key and sending said ballot request to the voting mediator.

21. The computer program product as described in of claim 20 further comprising the steps of:

- receiving said ballot request by the voting mediator;
- decrypting the encrypted ballot request with said voting mediator's private key;
- validating said voting entity's certificate; and
- authenticating and verifying the integrity of signed ballot request using the public key within said voting entity's certificate.

22. A computer program product in a computer readable medium for representing a person or group that will be voting over a computer network, the computer program product comprising:

- instructions for requesting an electronic voting ballot using a public key and a private key of said computer program product;

- instructions for receiving the requested electronic voting ballot for the purpose of voting in an election voting the computer network;

- instructions for receiving a vote on the electronic ballot, said voting being cast over a computer network; and

- instructions for sending said electronic ballot to be tabulated.

23. A computer program product in a computer readable medium for authorizing and creating anonymous electronic ballots for use in voting over a computer network, the computer program product comprising:

- instructions for receiving a ballot request;

- instructions for decrypting the ballot request;

- instructions for validating a voting certificate contained in the ballot request;

- instructions for crating an electronic ballot based on information contained in the ballot request; and

- instructions for sending a created electronic ballot to the source of the ballot request.

24. A computer program product in a computer readable medium for tabulating election results for an election in which electronic ballots, submitted over a computer network, are used, the computer program product comprising:

- instructions for receiving encrypted voting information containing an electronic ballot;

- instructions for decrypting the received encrypted voting information;

- instructions for validating the electronic ballot contained in the voting information; and

- instructions for incrementing vote totals to include votes of the electronic ballot contained in the received voting information.

25. A computer connectable to a distributed computing system including a process for voting electronically over said distributed system comprising:

- a processor;

- a native operating system to manage resources in the computing system;

- a client program for representing a person or group that will be voting in an election;

- a server program for authorizing and creating electronic voting ballots; and

- a second server program for receiving, validating and tabulating electronic voting ballots.

26. The computer as described in claim 25 wherein each of said client program, server and second server has a separate public key and private key.